Flinders UNIVERSITY

Williams, P.A.H. and Maeder, A.J. (2013). A conceptual framework for secure mobile health. Journal of the International Society for Telemedicine and eHealth, 1(1) pp. 44-51.

A CONCEPTUAL FRAMEWORK FOR SECURE MOBILE HEALTH

Patricia A. H. Williams PhD[1], Anthony J. Maeder PhD[2]

[1]eHealth Research Group, School of Computer and Security Science, Edith Cowan University, Joondalup, Western Australia
[2]School of Computing, Engineering & Mathematics, University of Western Sydney, Campbelltown, New South Wales, Australia

Abstract

Mobile health is characterised by its diversity of applicability, in a multifaceted and multidisciplinary healthcare delivery continuum. In an environment of rapid change with the increasing development of mobile health, issues related to security and privacy must be well thought out. The different competing tensions in the development of mobile health from the device technologies and associated regulation, to clinical workflow and patient acceptance, require a framework for security that reflects the complex structure of this emerging field. There are three distinct associated elements that require investigation: technology, clinical, and human factors. Each of these elements consists of multiple aspects and there are specific risk factors to be addressed successively and co-dependently in each case. The fundamental approach to defining a conceptual framework for secure use of mobile health requires systematic identification of properties for the tensions and critical factors which impact these elements. The resulting conceptual framework presented here can be used for new critique, augmentation or deployment of mobile health solutions from the perspective of data protection and security.

Keywords: telemedicine; mobile health; medical device; data security; privacy; risk management.

Introduction

Mobile health as an emergent area of health informatics is not yet clearly defined or well delineated according to such factors as its clinical process, environment of use, integration of device and service, or standardisation. This is due to its diversity of purpose such as mobile and remote patient monitoring, diagnostic and treatment devices, and the increasing rate of development of applications on personal mobile devices such as mobile telephones and tablet computers. Its breadth encompasses both clinical patient monitoring devices and the convergent technology space of personal communications and computing devices.

This diversity is reflected in the multiple competing descriptions of mobile health. Whilst mobile health has been defined as "emerging mobile communications and network technologies in healthcare"[1] and as “the integration of mobile devices into the practice of medicine”,[2] these definitions do not indicate the application or differentiation of the technology from other types of technology used to support healthcare.

Mobile health by default includes communication via wireless networks but does not exclusively have to use this communication medium, since many devices record and store information for download at a later point in time. However as communications technology becomes increasingly reliable, wireless communication methods are convenient and their use is often transparent to the user.

The most obvious benefit of mobile health is the accessibility to health related information in environments displaced from the normal desktop context. Further it provides new avenues to move healthcare monitoring from a clinical environment to the personal and/or home environment. This can be undertaken from the use of sophisticated monitoring devices as in the case of tele-monitoring of cardiac patients[3] to simple patient-managed smart phone camera photography in post-operative wound care management.[4]

The protection of healthcare information is important given the personalised and identifiable nature of health information. It is important to protect the confidentiality of information to ensure patient privacy

is not breached. Additionally, the integrity of healthcare information is fundamental given that it is the basis for clinical decisions and similarly, the availability of information, at the time it is required, is important if it is to be clinically useful in the decision making process. Thus, in a less controlled and complex mobile health environment, security, privacy and data protection are essential.

The challenge for healthcare is to embrace the potential of mobile health and not merely replicate current technologies into a wireless environment. Further, in addressing this challenge, the complexities of securing health information along a composite clinical information pathway and in each situation of use must be defined. This paper introduces a new perspective on the use of mobile health, using a deconstruction of the intrinsic elements of clinical, technology and human factors, coupled with a high level view of the security and privacy aspects that need consideration. Whilst the issues of confidentiality and privacy are vital, the issue of informed consent is beyond the scope of this paper.

A multifaceted and multidisciplinary continuum

There are various common design considerations that need to be raised and addressed in the use of mobile health. These include understanding the capability and potential of mobile devices both by the clinical community and by consumers of healthcare; the ease and accuracy of data capture and storage and transfer; the integration of data into existing health record systems; the review and management of such data including integration into existing workflow and decision-making processes; equitable and ubiquitous access to the technology; and the realistic usability of the devices and applications *in situ*. Ultimately the clinical continuity of care and the end-to-end use of information, from the information gained by remote monitoring through to the use of this information for clinical decision support, is perhaps the biggest challenge in this arena.

Given this complex mapping, it is useful to consider a deconstructed framework approach to identify the specific elements in designing any mobile health usage process. Figure 1 demonstrates a characteristic deconstruction/conceptual framework based on the three fundamental health information systems categories of 1-Technology, 2-Clinical and 3-Human Factors, which is proposed here as a mechanism to analyse and develop a risk based security framework for a balanced and effective approach to assessing design considerations for mobile health processes.

The construction of the proposed framework comes from knowledge of the area by the authors, supported by drawing from related literature. There are very few published articles or studies on mobile health and data protection and security. For instance a search in PubMed for “mobile health or mhealth and security and privacy” results in only 12 articles and only one article is of any depth in relation to the interface of processes and technology, as proposed in this paper. Hence the framework proposed here provides a fundamental basis for understanding and investigating this under researched area. The paper purposely categorises the factors in mobile health processes (as in figure 1) that are impacted by, or impact upon, security and privacy of health information. These factors are not ranked or assigned a relative importance as each process will be unique and the interplay of factors complex.

The complexity in tackling data protection and security, in any domain, means that framework approaches are commonly used to conceptualise processes in industry and in the health standards environment.[5-7] The adoption of a framework approach can provide a relevant and practical method to conceptualise, understand and analyse the application environment.

Competing tensions in framework

A frequent criticism of the implementation of health information systems is the lack of conceptualisation of the practical relevance and lack of a foundational conceptual design framework outside the adoption of the technology itself.[8] Figure 1 provides such a framework summarising the practical design considerations to address, such as ease of use (human factors), integration into workflow (clinical) and functional capacity of the platform (technology). It is within this framework that specific tensions between elements must now be identified, if subsequent analysis and adaption of security risk mitigations are

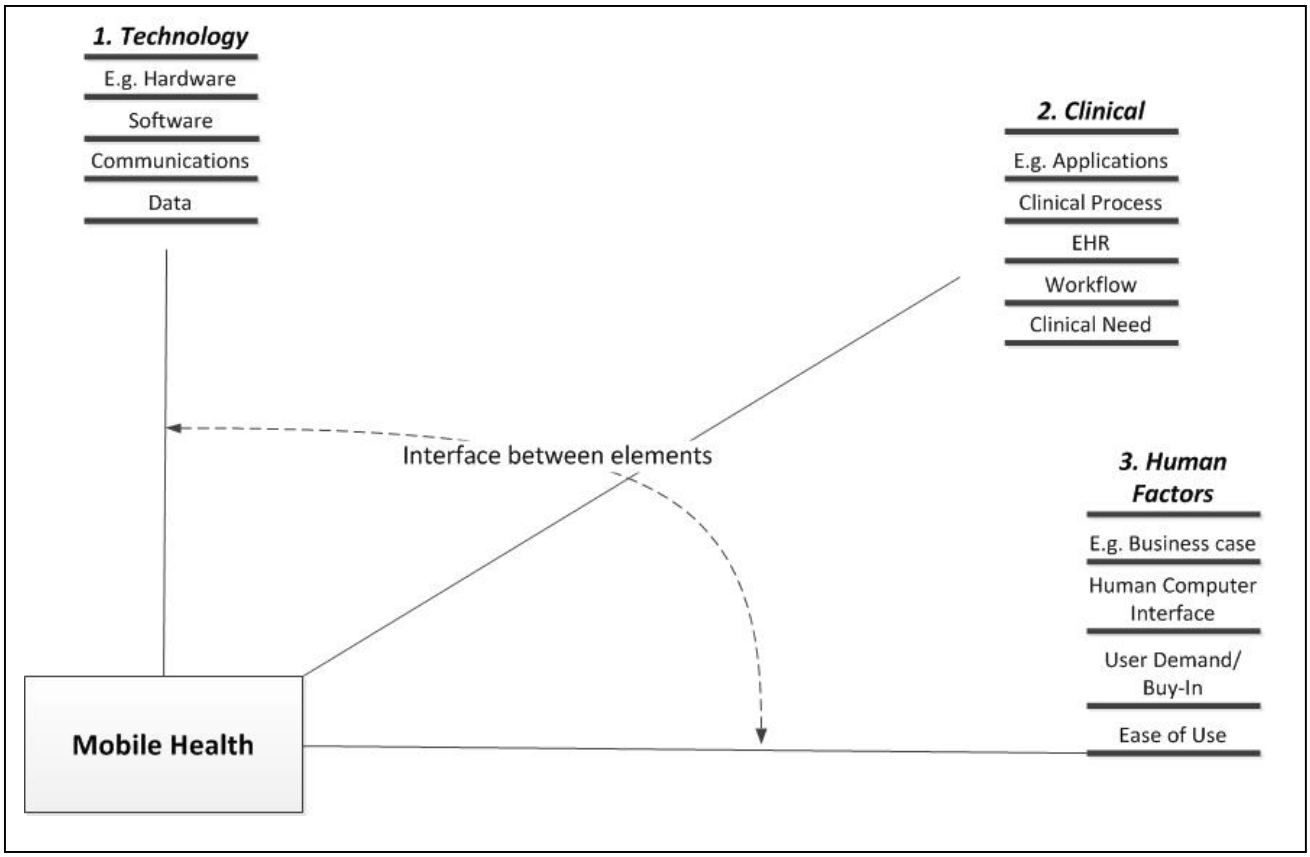

Figure 1. Deconstruction of mobile health process design elements

to be developed for practical application. It should be noted that the list of elements under each category is indicative and not exhaustive of the aspects that comprise mobile health processes. Whilst there are direct relationships between the categories and elements, these are dynamic and are not present between all elements, all the time. Each mobile health process will have an individual construction of elements on a case by case basis.

Technology tensions

There are numerous tensions in the technology element of mobile health. These exist across the spectrum of hardware, software, communications and data. Each of these aspects has its own security characteristics and implications for protection of healthcare information. In essence, this covers the factors of software incorporation into personal device security.

To date mobile health has been predominantly technology-based and with this comes the push for regulation based on the existing definitions of medical devices, heavily controlled by international standards. It may be inevitable that government oversight and regulation will impact upon this development.[9] In the USA for instance, where an application effectively transforms the mobile platform such as a smart phone or tablet computer, into a role with clinical applicability such as an electronic stethoscope, the device together with the application becomes a regulated medical device.[10] This tension is also being realised in the development of international standards such as *ISO 82304-1 Healthcare software systems - Part 1: General requirements* which looks at the safety associated with software systems and the crossover with medical devices. The tension exists

because this standard is related to healthcare devices and the influence that software has on standards processes for such previously 'specifically identifiable' medical devices.

This is a complex issue given that software now integrates seamlessly with smart personal devices to add functionality that enable them to achieve medical device utility. This is a well recognised issue in telemedicine, of which mobile health is closely aligned with.[11] "Regulation requires clear and careful definition of what is to be regulated" [12] and in a mobile health environment this is difficult as it fails to acknowledge the multifaceted, multi-technology and multidisciplinary boundaries that mobile solutions entail. Perhaps this dilemma is also due to the current debate on what the definition of mobile health should be. Similar debate exists around the definition and regulation of telemedicine. The questions of what should be regulated and in whose interests it should be regulated, still need to be answered.

In terms of software applications, what is currently lacking in the marketplace is any regulation of applications and a consequential lack of standardisation in software development and deployment.[10] As yet no legal precedents have been established in regard to this important issue. In contrast to the commonplace and relatively light impact wellness applications, there is perhaps more fundamental potential for risk in the development of new forms of clinical monitoring and treatment applications supported by mobile and particularly home monitoring equipment.

The activities of data capture and transfer also provoke issues that underpin much of the security considerations for the mobile health process. For these activities the models are generally based on one of three types: collection and aggregation of data, communication and interaction, and support applications such as self management.[13] In addition, the consideration of availability and communication paths is important from the technology perspective, as mobile communications are commonly enabled through Wi-Fi, Bluetooth, cellular and mobile phone communications or infrared signalling. Many devices can record information and then upload these data through web and Internet applications. Other than in critical care, this store and forward methodology is effective in many healthcare scenarios.

The risk to transfer of information using wireless technologies is not peculiar to healthcare. The risk of 'man in the middle' type attack (where data captured by an attacker through detecting and viewing data or by interrupting and modifying data) is present in any wireless network. Similarly 'denial of service' attack with the interruption of availability of services is another common security threat. The threats to confidentiality and patient privacy are often less severe concerns than the availability of information transfer in the wireless environment, particularly in emergency and time critical situations.

Lastly, an often overlooked issue is that of physical (hardware) durability and clinical infection control. Clearly, the concern regarding electromagnetic interference and therefore patient safety must be addressed,[14] and other physical concerns such as cross-infection, particularly when using mobile devices in a sensitive clinical setting. Whilst clinical devices and equipment are subject to a strict hygiene and sterilisation in the medical environment, it is doubtful whether computer hardware is subject to the same well established infection control protocols.[10]

Clinical tensions

Whilst there is a distinct and rapidly growing presence of mobile applications for preventative health for personal use,[15] there are relatively few which have been developed for direct clinical applicability. However, the demand on mobile health technologies by healthcare providers is reportedly set to increase rapidly over the next few years.[16] Such development aspirations need however to be tempered with concerns regarding data security.

The interference with healthcare process workflow and the clinical interaction between the patient and clinician has been cited as potential reasons for the slow adoption by clinicians of mobile health solutions.[2] Over time a change in work practice and social norms, driven by the adoption of technology by clinicians, will impact on the rate of adoption of mobile health, particularly as younger clinicians will be more comfortable with adopting mobile technologies and integrating these into clinical

practice.[17,18] Further, historically there has been concern over the hygiene and sterility of computer hardware and the introduction of mobile and potentially less sterile devices should be a consideration.

Therefore, integration into workflow is a major factor in the development of mobile health solutions, as is the integration of the data collected into existing health information systems. This is inclusive of the decision making responsibility and associated processes. Indeed, the redesign of healthcare processes, inclusive of critical impact factors such as policy, participant roles, stakeholder engagement and information systems usage, has been identified as fundamental to quality healthcare improvement.[19] Such redesign necessitates new models such as a 'patient journey' perspective to be adopted to maximise the effective integration of mobile health into conventional healthcare process.

The redesign also creates tensions in both its development, engagement of stakeholders, and effective implementation. Little research has been undertaken into data safety monitoring (DSM) for mobile health situations, given that DSM has traditionally been associated with the detection of adverse events and monitoring of new therapeutic devices. Consequently, it has been highlighted that practical advice is scarce on how to respond to critical alerts in real time and how to manage subsequent interventions (i.e. how to integrate monitoring into normal workflow).[20]

Similarly, by integration into existing systems, the volume of health and wellness applications (particularly on smart phones and devices such as iPads) have spawned a software application industry focusing on exercise, diet and other wellness related factors. This is of benefit to the patient in promoting healthier lifestyle and in encouraging responsibility for personal healthiness and involvement in their own healthcare.[7,10] Interestingly, many applications exist for recording personal electronic health records, although at present these are seldom able to be integrated into either primary care clinical systems or national personally controlled electronic health records (such as the Personally Controlled Electronic Health Record in Australia).

Human factors tensions

One of the major benefits of mobile health is the accessibility to accurate personal healthcare information in emergency situations where critical decisions need to be made rapidly. This is one area in which an understanding of the capabilities and potential by consumers is necessary, which requires education and engagement. However, as in any healthcare innovation, consideration of the equitable access to the level of care provided must be included. This may incorporate the cost of devices and communications coverage, a particular issue in rural and remote communities as well as developing World settings.

Similarly, the usability of devices and applications is an area of consideration and more commonly referred to as human computer interaction. Studies have shown[21] that acceptance of mobile devices at the point of care have been traditionally low. Indeed, Heeks' review[22] of the factors of design-reality gap influence in the success and failure of health information systems, demonstrates that user acceptance of new health information systems is not high given the history of trialled and failed systems.

Combined tensions

Mobile health is complex synergy of the technology, clinical use and human factors. Mobile health can present disruption to conventional healthcare processes in part due to the shift in responsibility and placement of diagnosis in the healthcare process workflow, and an increased focus on patient self-management.[23] This disruption can also be attributed to the vast amount of data that can be recorded in a variety of media using single convergent technology devices. From a security perspective these two disruptive factors create multiple complexities and require an understanding of the context of use, as well as the technological and workflow elements, in order to provide effective security of data and assurances to all actors (patients and healthcare providers) participating in the health care process.

Another major tension is the proof of clinical usefulness and efficacy in the use of the mobile healthcare delivery continuum. This issue is not restricted to the domain of mobile health, and has had

much discussion in the area of telehealth.[24] Indeed, the requirement for business case sustainability as well as assessment of clinical and economic benefit is a major factor in the clinical adoption and use of mobile health. The level of usefulness will be dependent upon clinical need and expectation.

A common problem both for clinicians and patients is the lack of security awareness in general,[25] particularly in relation to mobile devices.[14] This issue affects many aspects of the mobile health delivery continuum, and its integration into this continuum needs to be carefully addressed. The issue can both be highlighted by and addressed by design-reality gap inclusion, as discussed above.

Lastly, the issues of patient privacy and data confidentiality along the mobile health delivery continuum remain significant anxieties. The lack of control over the data collected, stored, and transferred over critical infrastructure, together with the provenance of data privacy across device, platforms and clinical information systems, should be a major cause for concern.[26]

Element risk factors

In the development of a comprehensive framework for security and privacy, the tensions described must be considered within a broader perspective of the end-to-end health information transfer and use, and the holistic health information system. If the mobile health process design elements, as in figure 1, are considered together with the integration of design-reality, this may contribute to practical security and privacy mobile solutions.

Whilst some privacy frameworks have been suggested,[27] most relate to the privacy of the individual monitoring and not cross-spectrum to the flow of mobile healthcare incorporating the three essential facets of technology, clinical and human factors. Furthermore, they are general principle frameworks and do not provide implementation assistance with which to support practical use. The important issue of provenance of data is rarely considered. This potentially reflects the complexity of defining such framework across different jurisdictions, countries and legal systems.

From a risk perspective, each element in the end-to-end delivery of healthcare using mobile devices can be independently assessed and mitigations devised. However, this is not necessarily the best or most effective perspective with which to look at the security solutions. The frequency and severity of threats and vulnerabilities, and the ability and feasibility to mitigate against these threats, also need to be considered. Therefore, applying the same approach to each element independently, for instance where human factors are high risk and technology factors are low risk, may result in ineffective solutions and unnecessary and costly mitigation strategies which could compromise the effectiveness of the clinical process. An understanding of the co-dependency of the risk factors needs to be present and the risk mitigations tailored accordingly.

Conclusion

As mobile devices become more pervasive and the acceptance of the technology increases, and as more health applications are produced, home based healthcare and personal health monitoring will become mainstream to health provision. Whilst adoption by clinicians is currently slow, there is recognition of the potential for mobile health to revolutionise healthcare delivery, beyond simple educational needs. The tensions identified above for each of the three identified elements in mobile health will help developers to formulate a risk based framework for protection of data, applicable along the entire end-to-end continuum for mobile health applications and their integration into clinical practice.

Whilst to date mobile health has been technology driven, the development of appropriate software applications and an increasing focus by international standards bodies (such as Health Level 7) is providing the recognition that mobile health and personal healthcare monitoring needs to have equal focus on behavioural processes if it is to be effectively and successfully adopted. These behavioural processes apply to both the receiver of healthcare and the providers of such service. Whilst useful in the personal context for health and wellness activities, a large part of the attractiveness of mobile health lies in the largely unexplored area of using this information in clinical decision support and providing better outcomes for patients.

The idea of fit and congruence is an important one. In a mobile health systems environment, the ability of the technology, software and its associated processes to adapt to change is important. Incorporating a predominantly matched (rather than mismatched) situation in design-reality helps to enable acceptance in reality and minimise the design-reality gap.[22] This is even more important where it relates to adaptation to the context of use, rather than actual use of the technology, no matter how good the application is. The fit between the technology and task in important, as is the fit of the technology and task to the context it is used in. This is reliant on avoiding changes to the environment and processes because of the use of the technology. What is more effective here as a design consideration is the seamless integration of the technology and process into an existing clinical utility workflow.

Further research in the development of a risk-linked mobile health framework is currently being undertaken. This work includes an in-depth perspective and all-inclusive detailed mapping of the specific issues for each of the deconstructed technology, clinical and human factor facets. The proposed framework provides a fundamental starting point from which to take a comprehensive yet innovative perspective on mobile health and modelling the security and privacy of the processes as well as the technology involved.

.....

Conflict of Interest. The authors declare no conflict of interest.

Corresponding Author:
P Williams,
eHealth Research Group,
School of Computer and Security Science,
Edith Cowan University,
Joondalup,
Western Australia
trish.williams@ecu.edu.au

References

1. Osunmuyiwa O, Ulusoy AH. Wireless security in mobile health. *Telemed J EHealth* 2012;18(10):810-814.
2. Sclafani J, Tirrell TF, Franko OI. Mobile tablet use among academic physicians and trainees. *J Med Syst* 2013;37(1):1.
3. Blazek N. Wireless technology is transforming the medical community. *Cardiology Today* 2012;15(7):1-11.
4. de Sain R. Mobile key in the dialogue of care. *PulseIT* 2011:36-37.
5. APQC. (2011). Using process frameworks and reference models to get real work done. Available at: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Using_Process_Frameworks_and_Reference_Models_to_Get_Real_Work_Done.pdf accessed 5 April 2013.
6. Campbell M, Fitzpatrick R, Haines A, et al. Framework for design and evaluation of complex interventions to improve health. *BMJ* 2000; 321(7262):694–696.
7. APEC (2005). Privacy framework. Available at: http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf accessed 5 April 2013.
8. Lorenzi NM, Smith JB, Conner SR, Campion TR. The success factor profile for clinical computer innovation. In: M. Fieschi EC, Y.-C.J. Li, editors. Medinfo 2004. Amsterdam: IOS Press; 2004;1077-1080.
9. Silberman MJ, Ciark L. M-Health: The union of technology and healthcare regulations. *J Med Pract Manage* 2012;28(2):118-120.
10. Ardito SC. Mobile apps for the health professional. *Searcher* 2011;19(6):46-50.
11. Imouokhome FA, Osubor VI. Mobile-device-based telemedicine for improved health-wealth. *African Journal of Computing & ICT (IEEE)* 2012;5(5):142-147.
12. Jack C, Mars M. Why is telemedicine a challenge to the regulators? *S Afr Bioethics Law* 2010;3(2):55-58.
13. Maeder AJ. Tablet computers for mHealth: Opportunities for personal healthcare. IASTED International Conference Health Informatics (AfricaHI 2012), 2012. Botswana, Africa. 355-359.
14. Brady RRW, Gibb AP, Visvanathan A. Increasing clinical presence of mobile communication technology: avoiding the pitfalls. *Telemed J EHealth* 2011;17(8):656-661.
15. Maliszewski SC. (2013). Certifying mobile health apps: Just what the doctor ordered. Available at: http://www.mhimss.org/news/certifying-mobile-health-apps-just-what-doctor-ordered accessed 20 February 2013.

16. Dunbrack LA. (2011). The second wave of clinical mobility: Strategic solution investments for mobile point of care. Available at: https://idc-insights-community.com/health/healthcare-transformation/the-second-wave-of-clinical-mobility-strategic-sol accessed 12 December 2012.
17. O'Brien MA, Rogers WA, Fisk AD. Understanding age and technology experience differences in use of prior knowledge for everyday technology interactions. *ACM Trans Access Comput* 2012;4(2):1-27.
18. Morris MG, Viswanath V. Age differences in technology adoption decisions: Implications for a changing work force. *Pers Psychol* 2000;53(2):375-403.
19. Curry J, McGregor C, Tracy S. A communication tool to improve the patient journey modeling process. 28th IEEE EMBS Annual International Conference 2006. New York City, USA. IEEE: 4726-30.
20 Aubrecht JA, Dabbs AD, Dew MA, Kovach KA, Myers B. Data safety and monitoring for research involving remote health monitoring. *Telemed J EHealth* 2011;17(7):574-579.
21. Reussa E, Menozzia M, Buchi M, Koller J, Krueger H. Information access at the point of care: what can we learn for designing a mobile CPR system? *Int J Med Inform* 2004;73(3) ;363-369.
22. Heeks R. Health information systems: Failure, success and improvisation. *Int J Med Inform* 2006;75(2):125-37.
23. Gogia SB, Maeder A, Meher S, Mars M, Hartvigsen G, Kuthiala A. Using personal handheld computing devices for personalizing healthcare.*Yearb Med Inform* 2012:74-8.
24. Maeder A, Gogia SB, Hartvigsen G. Next generation telehealth. Y*earbook Med Inform* 2011:15-20.
25. Williams PAH. When trust defies common security sense. *Health Informatics J* 2008;14(3):211-221.
26. Atienza AA, Patrick K. Mobile Health: The killer app for cyberinfrastructure and Consumer Health. *Am J Prev Med* 2011;40(5, Supplement 2):S151-S53.
27. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. *ACM Comput Surv* 2012;45(1):1-54.